APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/503,205	02/14/2000	Jun Kogure	826.1590/JDH	6229

21171 7590 05/19/2005	EXAMINER	
STAAS & HALSEY LLP	KLIMACH, PAULA W	
SUITE 700		
1201 NEW YORK AVENUE, N.W.	ART UNIT	PAPER NUMBER
WASHINGTON, DC 20005	2135	

DATE MAILED: 05/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/503,205	KOGURE, JUN
	Examiner	Art Unit
	Paula W. Klimach	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>02/14/05</u>.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 02/14/05 has been entered.

Response to Arguments

Applicant's arguments filed 02/14/2005 have been fully considered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 6-12, and 14-19 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Leppek (5,933,501) in view of Schneier.

In reference to claims 1, 8, and 11, Leppek suggests a data generating apparatus and

computer readable storage medium, comprising: an input device inputting a condition for

designating a finite field (column 4 lines 33-51); a generation device automatically generating

expression data of the finite field based on the inputted condition (column 4 lines 52-67); and an

expression data storage device storing the generated expression data (column 4 lines 7-23).

Although Leppek discloses a system that uses PGP (column 4 lines 14-17), Leppek does

not provide details that would indicate that the PGP algorithm whose conditions are of a finite

field corresponding to a mathematical finite aggregate in which four arithmetical operations are

defined, a number of elements of the finite aggregate being expressed as p^m with p and m as

prime number and a positive integer indicating an extension degree, respectively. In addition,

Leppek is silent on the origins of the key 170 and therefore a condition specified by a user.

Schneier discloses the details of the PGP algorithm (page 584), which includes IDEA.

The IDEA algorithm has S-boxes which have the condition are of a finite field corresponding to

a mathematical finite aggregate in which four arithmetical operations are defined, a number of

elements of the finite aggregate being expressed as p^m with p and m as prime number and a

positive integer indicating an extension degree, respectively (page 320 paragraph 2). Schneier

discloses the user entering a passphrase that is used as the conditions for the hash algorithm to

create the key (page 174 paragraphs 2-7).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use details of the PGP algorithm as disclosed by Schneier and have a user enter

the passphrase as disclosed in Schneier to enter the key that is disclosed by Leppek. One of

ordinary skill in the art would have been motivated to do this because Leppek does not disclose

the details of the PGP algorithm that is used as part of the invention while Schneier gives the

details and the user entered passphrase gives the user the ability to be as unpredictable as

possible.

In reference to claim 9, Leppek suggests a data generating method, comprising: designating a condition for designating a finite field (column 4 lines 33-51); automatically generating expression data of the finite field based on the designated condition (column 4 lines 52-67); and supplying the generated expression data to a finite field operation apparatus (column 4 lines 7-23).

Although Leppek discloses a system that uses PGP (column 4 lines 14-17), Leppek does not provide details that would indicate that the PGP algorithm whose conditions are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as $p^{\wedge}m$ with p and m as prime number and a positive integer indicating an extension degree, respectively.

Schneier discloses the details of the PGP algorithm (page 584), which includes IDEA. The IDEA algorithm has S-boxes which have the condition are of a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^{m} with p and m as prime number and a positive integer indicating an extension degree, respectively (page 320 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use details of the PGP algorithm as disclosed by Schneier. One of ordinary skill in the art would have been motivated to do this because Leppek does not disclose the details of the PGP algorithm that is used as part of the invention while Schneier gives the details.

In reference to claims 10 and 16, Leppek suggests a data generating apparatus, comprising: inputting means for inputting a condition for designating a finite field (column 4 lines 33-51); generating means for automatically generating expression data of the finite field

based on the inputted condition; and expression data storing means for storing the generated

expression data (column 4 lines 52-67).

Although Leppek discloses a system that uses PGP (column 4 lines 14-17), Leppek does

not provide details that would indicate that the PGP algorithm whose conditions are of a finite

field corresponding to a mathematical finite aggregate in which four arithmetical operations are

defined, a number of elements of the finite aggregate being expressed as $p^{\wedge}m$ with p and m as

prime number and a positive integer indicating an extension degree, respectively.

Schneier discloses the details of the PGP algorithm (page 584), which includes IDEA.

The IDEA algorithm has S-boxes which have the condition are of a finite field corresponding to

a mathematical finite aggregate in which four arithmetical operations are defined, a number of

elements of the finite aggregate being expressed as p^{m} with p and m as prime number and a

positive integer indicating an extension degree, respectively (page 320 paragraph 2).

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to use details of the PGP algorithm as disclosed by Schneier. One of ordinary skill

in the art would have been motivated to do this because Leppek does not disclose the details of

the PGP algorithm that is used as part of the invention while Schneier gives the details.

Claims 2-3, 6-7, 12, 14-15, and 17-19 are rejected as in claims 1 and 11.

Regarding claims 2, 12, and 17, further comprising an operation device performing a

finite field operation based on the expression data stored in said expression data storage device

(column 5 lines 34-52).

Regarding claims 3, 14, and 18, wherein when a bit length of a prime number which describes the finite field is inputted as the condition, said generation device automatically generates prime number data corresponding to the bit length and stores the generated prime number data in said expression data storage device. Leppek uses different encryption routines (column 4 lines 14-17) one well known example is the RSA encryption routine, which uses random keys. The size of the keys is a design choice. The keys are inherently developed using a random number generator, which would generate them automatically

Regarding claim 6, further comprising a fixed data storage device storing one or more pieces of predetermined expression data of a finite field (Fig. 2), said generation device stores expression data of a finite field corresponding to the condition in said expression data storage device if there is the expression data of a finite field corresponding to the condition in the fixed data storage device, and said generation device automatically generates expression data of a finite field corresponding to the condition if there is no expression data of a finite field corresponding to the condition in the fixed data storage device (column 5 lines 6-18). The generator, of the Leppek system, always constructs the expression from the access code data using the stored information in the fixed storage such as 100.

Regarding claims 7, 15, and 19, further comprising: a designation device designating expression data of a finite field (column 5 lines 6-18); and a verifier device verifying whether the designated expression data are suitable, the verifier device sores designated expression data in said expression data storage device if the designated expression data are suitable, and the verifier device asks the designation device for other expression data if the designated expression data are not suitable (claim 5 lines 19-33). The supervisory encryption assembly manager processes the

sequence and therefore is responsible for verifying that the encryption process is carried out as designed.

Claims 4, 5, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leppek as applied to claim 1 above, and further in view of Wright.

Leppek does not expressly disclose the generation of polynomial expressions

Regarding claims 4 and 13, Wright discloses a random polynomial generator wherein when an extension degree which describes the finite field is inputted as the condition, said generation device automatically generates irreducible polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device (part 2.1 page 2).

Regarding claim 5, The data generating apparatus according to claim 4, wherein when an instruction using an optimal normal basis is inputted, said generation device automatically generates irreducible polynomial data for an optimal normal basis corresponding to the extension degree and the irreducible polynomial data for an optimal normal basis in said expression data storage device. Leppek discloses storing the predetermined expression in storage 100, however Leppek does not expressly disclose the generation of polynomial expressions. Wright discloses the generation of polynomial expressions (part 2.1 page 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the polynomial generator as in Wright in the system of Leppek. One of ordinary skill in the art would have been motivated to do this because Leppek discloses the use of conventional encryption algorithms (column 4 lines 14-17) and Wright discloses a polynomial generator which is satisfactory and has already been proven (Introduction 1 page 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854.

The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Monday, May 16, 2005

AU 2135